(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

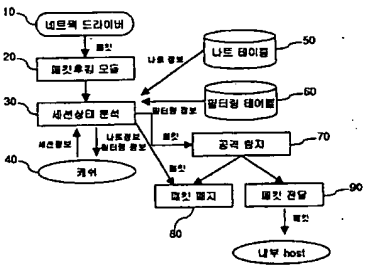
(11)Publication number: 1020020086434 A
(43)Date of publication of application: 18.11.2002

(21)Application number: 1020020065296
(22)Date of filing: 24.10.2002
(51)Int. Cl H04L 12 /22

(71)Applicant: CENTAVISION CORP.
(72)Inventor: PARK, GEUN DEOK

(54) HACKING CONTROL SYSTEM

(57) Abstract:



PURPOSE: A hacking control system is provided to embody a firewall system for grasping whether a service of an inputted packet is admitted and transmitting a packet to an other internal computer and a hacking preventing system for preventing that a packet is retrieved and the internal computer is hacked or attacked by one body, and control a hacking. CONSTITUTION: A packet hooking module (20) hooks a packet inputted through a network. A session state analyzing module(30) retrieves whether a session about a starting place host designated by information included in the packet hooked in the packet hooking module(20), changes information recorded in the session, and judges whether a service requested by the starting place host is admitted. An attack detecting module(70) analyzes the packet hooked in the packet hooking module(20), and detects a hacking or attack attempt. A packet discard module(80) discards a packet which is judged that a no-admission service is requested in the session state analyzing module(30) or is harmfully judged in the attack detecting module(70). A transmitting module(90) transmits a packet harmlessly judged in the attack detecting module(70) to an internal destination host according to session information associated with the packet.

Legal Status
Date of request for an examination (20021024)
Notification date of refusal decision (00000000)
Final disposal of an application (registration)
Date of final disposal of an application (20040129)
Patent registration number (1004194720000)
Date of registration (20040209)
Number of opposition against the grant of a patent ( )

Date of opposition against the grant of a patent (00000000)

Number of trial against decision to refuse ( )

Date of requesting trial against decision to refuse ( )

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04L 12/22

(11) 공개번호 특2002 -0086434
(43) 공개일자 2002년11월18일

(21) 출원번호 10 -2002 -0065296
(22) 출원일자 2002년10월24일

(71) 출원인 (주)센타비전
부산광역시 남구 대연6동 1775 -25 3/1 2F

(72) 발명자 박근덕
부산광역시남구대연6동1775 -253통1반

(74) 대리인 구성진

심사청구 : 있음

(54) 침입통제시스템

요약

본 발명은 컴퓨터 운영체계의 네트워크 드라이버에 포함되어 침입탐지와 방어가 이루어지는 침입통제시스템에 관한 것으로 보다 상세하게는 네트워크를 통해 입력되는 패킷을 후킹하는 패킷후킹모듈;과 상기 패킷후킹모듈에서 후킹된 패킷에 포함된 정보로 특정되는 출발지호스트에 대한 세션이 존재하는지 검색하고, 상기 세션의 상태정보를 변경하며, 상기 세션에 기록된 정보에 따라 상기 출발지호스트가 요청한 서비스가 허용되는지 판단하는 세션상태분석모듈;과 상기 패킷후킹모듈에서 후킹된 패킷을 분석하여 침입 또는 공격 시도를 탐지하게 되는 공격탐지모듈;과 상기 세션상태분석모듈에서 허가되지 않은 서비스를 요청한 것으로 판단되거나 상기 공격탐지모듈에서 유해한 것으로 판정된 패킷을 폐기하는 패킷폐기모듈;과 상기 공격탐지모듈에서 무해한 것으로 판정된 패킷을 상기 패킷과 관련된 상기 세션정보에 따라 내부의 목적지호스트로 전달하게 되는 전달모듈;을 포함하여 구성되어 컴퓨터 운영체계의 커널의 네트워크드라이버에 삽입되며 상기 네트워크드라이버로 입력된 패킷을 후킹하여 필터링하는 것을 특징으로 하는 침입통제시스템에 관한 것이다.

이에따라 방화벽의 역할과 침입탐지 및 방어가 함께 이루어져 패킷의 분석이 효율적으로 처리되며 능동적인 방어가 가능하여 네트워크보안효과가 높아지게된다.

대표도
도 1

색인어

침입탐지 패킷, 아이피 에이알피 나트

명세서

도면의 간단한 설명

도1 : 본 발명의 일실시예에 따른 침입통제시스템의 블럭도

도2 : 본 발명의 일실시예에 따른 침입통제시스템의 흐름도

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크의 보안 시스템에 관한 것으로 보다 상세하게는 입력된 패킷의 서비스 허용여부를 파악하여 내부의 타 컴퓨터로 패킷을 전달하는 방화벽시스템과 패킷을 검색하여 내부의 컴퓨터에 침입하고자 하거나 공격을 하고자 하는 것을 방지하는 침입방지 시스템이 일체화되어 침입을 통제하는 시스템에 관한 것이다.

일반적으로 네트워크에 연결된 호스트는 외부에서 쉽게 접근할 수 있으므로 외부로부터의 침입 또는 공격에 의해 내부에 저장된 자료가 유출되거나 파괴되어 큰 피해가 발생하게 된다. 이러한 외부로부터의 공격을 방어하기 위해 내부의 네트워크와 외부의 네트워크사이에 방화벽을 설치하여 허용되지 않은 접속은 거부되어 접속이 차단된다.

그러나 상기 방화벽은 단순히 접속의 허용여부만을 테이블에서 검색하여 처리하므로 접속이 허용된 것처럼 위장하여 접근하는 경우 쉽게 내부 네트워크로 연결된다는 문제점이 있다.

이러한 문제점을 해결하기 위해 외부에서 입력된 패킷을 분석하여 공격 또는 침입시도를 판단하여 능동적으로 방어하는 침입탐지시스템을 도입하고 있다. 상기 침입탐지시스템은 패킷의 수집, 데이터 축약, 패킷분석, 공격탐지의 단계를 통해 사전에 파악된 공격방법과 현재 입력된 패킷을 비교하여 상대의 의도를 파악하여 유해한 접속을 차단하게 된다.

기존에는 상기 방화벽 또는 침입탐지시스템을 별도로 설치하거나 하나의 호스트 내에 각각의 방화벽시스템과 침입탐지시스템 소프트웨어를 설치하여 방화벽과 침입탐지가 순차적으로 이루어지도록 구성되었다.

그러나 상기와 같이 별도의 시스템을 구성하거나 각각의 소프트웨어를 설치하여 보안시스템을 구축하는 경우 방화벽과 침입탐지가 별도로 이루어지므로 패킷의 처리효율이 떨어지며 과다한 도입비용이 들어가게 된다는 문제가 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 문제점들을 해결하기 위해 안출된 것으로 운영체계의 커널의 네트워크 드라이버에 포함되어 방화벽의 역할과 침입탐지가 동시에 이루어져 도입비용이 저렴하면서도 패킷의 분석이 효율적으로 이루어져 능동적인 방어가 가능한 네트워크 보안 시스템을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

본 발명은 네트워크를 통해 입력되는 패킷을 후킹하는 패킷후킹모듈;과 상기 패킷후킹모듈에서 후킹된 패킷에 포함된 정보로 특정되는 출발지호스트에 대한 세션이 존재하는지 검색하고, 상기 세션의 상태정보를 변경하며, 상기 세션에 기록된 정보에 따라 상기 출발지호스트가 요청한 서비스가 허용되는지 판단하는 세션상태분석모듈;과 상기 패킷후킹모듈에서 후킹된 패킷을 분석하여 침입 또는 공격 시도를 탐지하게 되는 공격탐지모듈;과 상기 세션상태분석모듈에서 허가

되지 않은 서비스를 요청한 것으로 판단되거나 상기 공격탐지모듈에서 유해한 것으로 판정된 패킷을 폐기하는 패킷폐기모듈;과 상기 공격탐지모듈에서 무해한 것으로 판정된 패킷을 상기 패킷과 관련된 상기 세션정보에 따라 내부의 목적지호스트로 전달하게 되는 전달모듈;을 포함하여 구성되어 컴퓨터 운영체계의 커널의 네트워크드라이버에 삽입되며 상기 네트워크드라이버로 입력된 패킷을 후킹하여 필터링하는 것을 기술적 요지로 한다.

바람직하게는 상기 세션의 정보는 캐쉬에 저장되는 것이 바람직하다.

바람직하게는 상기 컴퓨터 운영체계의 커널의 네트워크드라이버는, 오에스아이레이어 3계층의 아이피 내지 에이알피 드라이버가 되는 것을 다른 기술적 요지로 한다.

바람직하게는 상기 세션상태분석모듈은, 새로운 세션이 생성되는 세션생성모듈;과 출발지호스트의 아이피내지 에이알피정보와 필터테이블을 비교검색하여 상기 출발지호스트에서 요청한 서비스의 허용여부를 세션에 기록하게되는 서비스검색모듈;과 나트테이블을 검색하여 세션에 나트정보를 추가하는 나트테이블검색모듈;을 포함하여 구성되어 세션이 존재하지 않거나 정보가 없는 세션을 처리하는 것을 또 다른 기술적 요지로 한다.

이하에서는 첨부된 도면을 참조로하여 본 발명의 일실시예에 따른 침입통제시스템에 대해 상세하게 설명하기로 한다.

도1은 본 발명의 일실시예에 따른 침입통제시스템의 블럭도이며, 도2는 본 발명의 일실시예에 따른 침입통제시스템의 흐름도이다.

본 발명의 일실시예에 따른 침입통제시스템은 크게 패킷후킹모듈(20), 세션상태분석모듈(30), 공격탐지모듈(70), 패킷폐기모듈(80),전달모듈(90)로 나눌 수 있다.

먼저 패킷후킹모듈(20)에 대해 설명하기로 한다.

일반적으로 네트워크를 통해 데이터를 전송하기위해서 데이터의 묶음인 패킷을 사용하게 된다. 즉 데이터를 연속적으로 전송하는 대신 적당한 크기로 나누어 패킷의 형태로 구성한 다음 패킷들을 하나씩 보내는 방법을 쓴다. 각각의 패킷은 일정한 크기의 데이터뿐만 아니라 도착지와 출발지의 주소 또는 제어 부호 등의 제어 정보를 포함하게 된다. 상기 패킷은 물리적인 네트워크 장비를 통해 전달되어 호스트내에서 오에스아이계층을 따라 처리된다.

상기 패킷후킹모듈(20)은 상기 패킷이 오에스아이 3계층에 속하는 아이피 또는 에이알피 드라이버(10)로 전달되면 상기 패킷을 가로채어 후술하게 될 세션상태분석모듈(30)로 전달하게된다. 패킷의 후킹에 관한 기술은 당업계에서는 공지공용의 기술이므로 상세한 설명은 생략하기로 한다.

세션상태분석모듈(30)은 상기 패킷후킹모듈(20)에서 가로채어 전달한 패킷에 포함된 출발지의 주소와 도착지의 주소등의 주소정보에 대해 기존 생성된 세션들을 검색하게 된다. 여기서 상기 세션은 호스트간의 연결을 위한 논리적인 연결로서 출발지의 주소와 도착지의 주소와 상기 세션에 의한 통신이 허용되었는지 여부와 상기 도착지의 주소에 대한 나트테이블(50)상의 나트정보등의 세션에 관련된 정보를 캐쉬(40)에 저장하게 된다.

검색결과 해당 세션이 존재하지 않으면 후술하게 될 세션생성모듈을 호출하게 된다. 상기 세션생성모듈은 상기 세션상태분석모듈(30)로부터 출발지와 도착지의 주소를 전달받아 새로운 세션을 생성하게 된다. 세션의 생성에 관한 것은 당업자에게는 주지의 기술이므로 상세한 설명은 생략하기로 한다.

해당 세션이 존재하면 상기 세션상태분석모듈(30)은 캐쉬(40)로부터 상기 세션에 관련된 정보를 읽어 상기 세션에 대한 통신의 허용여부를 파악하게 된다. 이때 상기 세션에 대한 통신의 허용여부가 저장되어 있지 않을 경우 서비스검색모듈을 호출하여 통신의 허용여부를 파악하게 된다. 여기서 통신이 허용된 세션의 패킷은 나트정보를 확인한 후 공격탐지모듈(70)로 전달된다.

다음으로 서비스검색모듈을 설명하기로 한다. 상기 서비스검색모듈은 상기 세션생성모듈에서 새로 생성된 세션 또는 통신의 허용여부가 저장되어 있지 않은 세션에 대해 별도로 구비된 필터링테이블(60)을 참조로 하여 통신의 허용여부를 파악하게된다. 여기서 상기 필터링테이블(60)에는 출발지와 도착지의 주소, 그리고 패킷이 사용하는 포트등에 따라 통신서비스를 허용할 것인지 아니면 거부할 것인가의 여부가 저장되는 것이 바람직하다. 파악된 통신 허용여부는 상기 캐쉬(40)에 저장된 세션의 정보에 입력되어 이후 입력되는 패킷에 대해 상기 캐쉬(40)의 정보를 참조하여 허용여부를 판단하도록 구성된다.

다음으로 나트테이블검색모듈에 대해 설명하기로 한다. 상기 나트테이블 검색모듈은 캐쉬(40)에 저장된 세션의 정보에 나트정보가 포함되어 있지 않을 경우 호출되어 나트테이블(50)을 검색하여 패킷을 전달할 내부의 컴퓨터를 파악하게 된다. 파악된 나트정보도 상기 통신허용 여부와 같이 상기 세션의 정보에 저장되어 이후 상기 세션에 대한 패킷이 입력되면 캐쉬(40)에서 처리되도록 구성된다.

다음으로 공격탐지모듈(70)에 대해 설명하기로 한다. 상기 공격탐지모듈(70)은 패킷을 분석하여 호스트 또는 내부의 컴퓨터를 공격 내지 침입 시도를 파악하게 된다. 상기 공격탐지모듈(70)은 다양한 공격 내지 침입 시도방법의 패턴을 저장하여 입력된 상기 패킷과 상기 패턴을 비교하여 공격여부를 탐지하게 된다. 상기와 같은 공격탐지방법은 당업계에서 다양한 방법이 공지되어 있으므로 상세한 설명은 생략하기로 한다.

다음으로 패킷폐기모듈(80)에 대해 설명하기로 한다. 상기 세션상태분석모듈(30)에서 허용되지 않은 통신을 요청한 세션 또는 상기 공격탐지모듈(70)에서 공격 내지 침입을 시도한 패킷을 삭제하여 내부의 컴퓨터를 보호하게 된다.

다음으로 패킷전달모듈(90)에 대해 설명하기로 한다. 상기 세션에 저장되어있는 나트정보에 따라 해당 컴퓨터로 패킷을 전달하여 통신이 이루어지도록 하게된다.

상기의 패킷폐기와 패킷전달에 관한 기술은 네트워크의 보안에 관련된 당업계에서 널리 공지된 기술이므로 상세한 설명은 생략하기로 한다.

따라서 한번의 패킷수집으로 방화벽시스템과 침입탐지가 동시에 이루어지며, 전달된 패킷에 대한 세션이 존재하고 세션내에 정보가 있을 경우 상기 세션생성모듈과 서비스검색모듈과 나트테이블검색모듈을 호출하지 않고 상기 세션의 정보를 캐쉬에서 추출하여 비교하게 되므로 패킷의 처리시간이 단축되는 것을 알 수 있다.

발명의 효과

이에따라 본 발명에 의하면 네트워크 드라이버내에 방화벽과 침입탐지기능이 포함되어 패킷의 분석이 효율적으로 이루어져 능동적인 방어가 가능한 네트워크보안을 이루게 되며, 도입비용이 절감된다는 이점이 있다.

(57) 청구의 범위

청구항 1.

네트워크를 통해 입력되는 패킷을 후킹하는 패킷후킹모듈;과

상기 패킷후킹모듈에서 후킹된 패킷에 포함된 정보로 특정되는 출발지호스트에 대한 세션이 존재하는지 검색하고, 상기 세션에 기록된 정보를 변경하며, 상기 세션에 기록된 정보에 따라 상기 출발지호스트가 요청한 서비스가 허용되는지 판단하는 세션상태분석모듈;과

상기 패킷후킹모듈에서 후킹된 패킷을 분석하여 침입 또는 공격 시도를 탐지하게 되는 공격탐지모듈;과

상기 세션상태분석모듈에서 허가되지 않은 서비스를 요청한 것으로 판단되거나 상기 공격탐지모듈에서 유해한 것으로 판정된 패킷을 폐기하는 패킷폐기모듈;과

상기 공격탐지모듈에서 무해한 것으로 판정된 패킷을 상기 패킷과 관련된 상기 세션정보에 따라 내부의 목적지호스트로 전달하게 되는 전달모듈;을 포함하여 구성되어 컴퓨터 운영체계의 커널의 네트워크드라이버에 삽입되며 상기 네트워크드라이버로 입력된 패킷을 후킹하여 필터링하는 것을 특징으로 하는 침입통제시스템.

청구항 2.

제1항에 있어서 상기 세션의 정보는

캐쉬에 저장되는 것을 특징으로 하는 침입통제시스템.

청구항 3.

제1항에 있어서 상기 세션상태분석모듈은,

새로운 세션이 생성되는 세션생성모듈;과

출발지호스트의 아이피내지 에이알피정보와 필터테이블을 비교검색하여 상기 출발지호스트에서 요청한 서비스의 허용여부를 세션에 기록하게되는 서비스검색모듈;과

나트테이블을 검색하여 세션에 나트정보를 추가하는 나트테이블검색모듈;을 포함하여 구성되어 세션이 존재하지 않거나 정보가 없는 세션을 처리하는 것을 특징으로 하는 침입통제시스템.

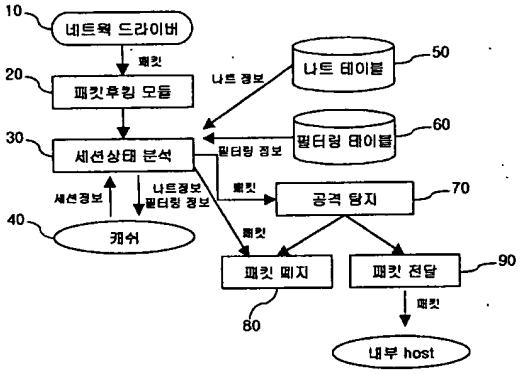
청구항 4.

제1항에 있어서 상기 컴퓨터 운영체계의 커널의 네트워크드라이버는,

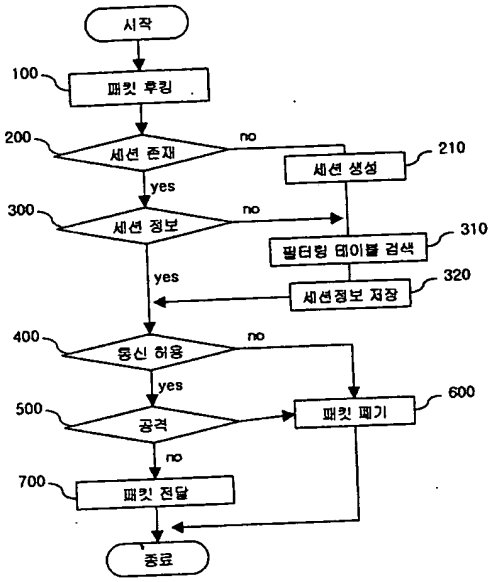
오에스아이레이어 3계층의 아이피 내지 에이알피 드라이버가 되는 것을 특징으로하는 침입통제시스템.

도면

도면 1



도면 2


시작
100
패킷 후킹
200
세션 존재
no
210
세션 생성
yes
300
세션 정보
no
310
필터링 테이블 검색
yes
320
세션정보 저장
400
통신 허용
no
yes
500
공격
600
패킷 폐기
no
700
패킷 전달
종료